ELEMENTÄR TALTEORI

4. RÄKNEÖVNINGARNA

Några studerande har frågat om det vore möjligt att få svårare problem. Några andra klagade, att problemen var får svåra. Därför är problem 1 lättare än tidigare, och problem 6 svårare än tidigare. I alla fall är inget problem omöjligt att lösa. :)

(1) Hitta ett reducerat restsystem modulo 30.
(2) Hitta primitiva rötterna modulo 11, och ordningen hos alla talen i det reducerade restsystemet modulo 11.
(3) Hitta polynomets $x^2 - x$ rötter modulo 5, och modulo 6. Varför är resultatet inte en kontradiktion mot Lagranges sats?
(4) Bevisa Wilsons sats, alltså visa att om p är ett primtal, då gäller
$$(p-1)! \equiv -1 \pmod{p}.$$
(5) Bevisa den andra sidan i Wilsons sats: Om
$$(n-1)! \equiv -1 \pmod{n},$$
är talet n ett primtal.
(6) Bevisa att det finns oändligt många primtal av form $4k + 3$. (Tipps: Hur visade vi att det finns oändligt många primtal? Är det möjligt att bearbeta beviset?)